

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Yutaka NAGAO

GAU:

SERIAL NO: NEW APPLICATION

EXAMINER:

FILED: HERewith

FOR: INFORMATION PROCESSING APPARATUS, INFORMATION PROCESSING METHOD, AND
INFORMATION PROCESSING SYSTEM

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e): Application No. Date Filed
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

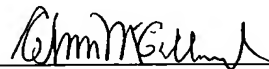
<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2003-142593	May 20, 2003

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)
- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle

Registration No. 40,073

C. Irvin McClelland
Registration Number 21,124

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 5 月 2 0 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 1 4 2 5 9 3
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 1 4 2 5 9 3]

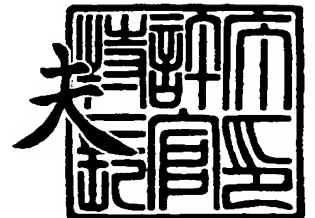
出 願 人 ソニー株式会社
Applicant(s):



2 0 0 4 年 2 月 2 3 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 0390279803

【提出日】 平成15年 5月20日

【あて先】 特許庁長官 殿

【国際特許分類】 G10L 5/04

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 長尾 豊

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100067736

【弁理士】

【氏名又は名称】 小池 晃

【選任した代理人】

【識別番号】 100086335

【弁理士】

【氏名又は名称】 田村 榮一

【選任した代理人】

【識別番号】 100096677

【弁理士】

【氏名又は名称】 伊賀 誠司

【手数料の表示】

【予納台帳番号】 019530

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707387

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置及び情報処理方法、並びに情報処理システム

【特許請求の範囲】

【請求項 1】 ライセンス情報に記された使用条件の範囲内でコンテンツ情報を使用可能な情報処理装置において、

第 1 のライセンス情報を保存する保存手段と、

第 2 のライセンス情報を受信する受信手段と、

第 1 のライセンス情報に対して第 2 のライセンス情報の一部又は全部を結合する結合手段とを有し、

前記結合手段により結合されたライセンス情報の範囲内でコンテンツ情報を使用することを特徴とする情報処理装置。

【請求項 2】 前記第 2 のライセンス情報は自身が上書きのためのライセンス情報であるか、追加のためのライセンス情報であることを識別させるライセンス識別情報を含むことを特徴とする請求項 1 記載の情報処理装置。

【請求項 3】 前記第 2 のライセンス情報が上書きのためのライセンス情報であることを前記ライセンス識別情報から確認したとき、前記結合手段は前記第 2 のライセンス情報の一部又は全部を前記第 1 のライセンス情報の一部又は全部に上書きすることを特徴とする請求項 2 記載の情報処理装置。

【請求項 4】 前記第 2 のライセンス情報が追加のためのライセンス情報であることを前記ライセンス識別情報から確認したとき、前記結合手段は前記第 1 のライセンス情報に対して前記第 2 のライセンス情報の一部又は全部を追加することを特徴とする請求項 2 記載の情報処理装置。

【請求項 5】 前記結合手段により結合されたライセンス情報に対して情報処理装置固有の鍵情報を用いて電子署名を行うことを特徴とする請求項 1 記載の情報処理装置。

【請求項 6】 前記第 1 のライセンス情報及び前記第 2 のライセンス情報が期間制限を指定する権利内容を含み、前記第 2 のライセンス情報が追加のためのライセンス情報であることを前記ライセンス識別情報から確認したとき、前記結合手段は前記第 1 のライセンス情報の権利内容に基づいた規則により前記第 1 のラ

イセンス情報と第 2 のライセンス情報とを結合することを特徴とする請求項 2 記載の情報処理装置。

【請求項 7】 前記第 1 のライセンス情報及び前記第 2 のライセンス情報がフラグを指定する権利内容を含み、前記第 2 のライセンス情報が追加のためのライセンス情報であることを前記ライセンス識別情報から確認したとき、前記結合手段は前記第 1 のライセンス情報の権利内容に基づいた規則により前記第 1 のライセンス情報と第 2 のライセンス情報とを結合することを特徴とする請求項 2 記載の情報処理装置。

【請求項 8】 前記第 1 のライセンス情報及び前記第 2 のライセンス情報が回数を指定する権利内容を含み、前記第 2 のライセンス情報が追加のためのライセンス情報であることを前記ライセンス識別情報から確認したとき、前記結合手段は前記第 1 のライセンス情報の権利内容に基づいた規則により前記第 1 のライセンス情報と第 2 のライセンス情報とを結合することを特徴とする請求項 2 記載の情報処理装置。

【請求項 9】 ライセンス情報に記された使用条件の範囲内でコンテンツ情報を使用可能とする情報処理方法において、

第 1 のライセンス情報を保存する保存工程と、

第 2 のライセンス情報を受信する受信工程と、

前記受信工程で受信した第 2 のライセンス情報が上書きのためのライセンス情報であるか、追加のためのライセンス情報であるかを識別させるライセンス識別情報から上書き又は追加属性を判別する判別工程と、

前記判別工程で判別した上書き又は追加属性に応じて第 1 のライセンス情報に対して第 2 のライセンス情報の一部又は全部を結合する結合工程とを有し、

前記結合工程により結合されたライセンス情報の範囲内でコンテンツ情報を使用することを特徴とする情報処理方法。

【請求項 10】 前記判別工程が前記ライセンス識別情報から前記第 2 のライセンス情報が上書きのためのライセンス情報であることを判別したとき、前記結合工程は前記第 2 のライセンス情報の一部又は全部を前記第 1 のライセンス情報の一部又は全部に上書きすることを特徴とする請求項 9 記載の情報処理方法。

【請求項 1 1】 前記判別工程が前記ライセンス識別情報から前記第 2 のライセンス情報が追加のためのライセンス情報であることを判別したとき、前記結合手段は前記第 1 のライセンス情報に対して前記第 2 のライセンス情報の一部又は全部を追加することを特徴とする請求項 9 記載の情報処理方法。

【請求項 1 2】 前記第 1 のライセンス情報及び前記第 2 のライセンス情報が期間制限を指定する権利内容を含み、前記判別工程が前記第 2 のライセンス情報が追加のためのライセンス情報であることを前記ライセンス識別情報から判別したとき、前記結合工程は前記第 1 のライセンス情報の権利内容に基づいた規則により前記第 1 のライセンス情報と第 2 のライセンス情報とを結合することを特徴とする請求項 9 記載の情報処理方法。

【請求項 1 3】 前記第 1 のライセンス情報及び前記第 2 のライセンス情報がフラグを指定する権利内容を含み、前記判別工程が前記第 2 のライセンス情報が追加のためのライセンス情報であることを前記ライセンス識別情報から判別したとき、前記結合工程は前記第 1 のライセンス情報の権利内容に基づいた規則により前記第 1 のライセンス情報と第 2 のライセンス情報とを結合することを特徴とする請求項 9 記載の情報処理方法。

【請求項 1 4】 前記第 1 のライセンス情報及び前記第 2 のライセンス情報が回数を指定する権利内容を含み、前記判別工程が前記第 2 のライセンス情報が追加のためのライセンス情報であることを前記ライセンス識別情報から判別したとき、前記結合工程は前記第 1 のライセンス情報の権利内容に基づいた規則により前記第 1 のライセンス情報と第 2 のライセンス情報とを結合することを特徴とする請求項 9 記載の情報処理方法。

【請求項 1 5】 第 1 のライセンス情報を保存する保存手段と、第 2 のライセンス情報を受信する受信手段と、第 1 のライセンス情報に対して第 2 のライセンス情報の一部又は全部を結合する結合手段とを有し、前記結合手段により結合されたライセンス情報の範囲内でコンテンツ情報を使用するクライアントと、

前記クライアントからの要求に応じて前記第 2 のライセンス情報をネットワークを通して送信するサーバと

を備えることを特徴とする情報処理システム。

【発明の詳細な説明】**【0 0 0 1】****【発明の属する技術分野】**

本発明は、情報処理装置及び情報処理方法並びに情報処理システムに関し、特に著作権者から付与されるライセンス情報に記された使用条件の範囲内でコンテンツ情報を使用可能な情報処理装置及び情報処理方法並びに情報処理システムに関する。

【0 0 0 2】**【従来の技術】**

インターネット等のネットワークを経由して、音楽・映像等のデジタルコンテンツを購入するサービスが普及している。例えば、インターネットを利用した音楽配信サービス（Electronic Music Distribution：EMD）を利用すれば、デジタル音楽コンテンツをダウンロードしてクライアント端末であるパーソナルコンピュータに保存し、パーソナルコンピュータ上で聞くことができる。

【0 0 0 3】

このとき、パーソナルコンピュータ側では、所定の著作権保護技術を採用した音楽記録再生アプリケーションをOSの基に起動し、暗号化したデジタルコンテンツを含むコンテンツファイルとそれに対応する利用条件を記述した権利ファイルをHDD等に格納してセキュアなサービスを実現していた。

【0 0 0 4】

本件出願人による特開平14-359616号公報には、所定の著作権保護技術を採用した音楽記録再生アプリケーションを起動することによってコンテンツの流通を妨げることなく、不正に利用されることを確実に防止することを目的とした情報処理装置等が開示されている。

【0 0 0 5】**【特許文献1】**

特開平14-359616号

【0 0 0 6】**【発明が解決しようとする課題】**

ところで、あるデジタルコンテンツに対応する権利情報は一種類とは限らず、また一種類だとしても同一デジタルコンテンツに対して、複数の権利情報ファイルを取得することが可能である。

【0007】

クライアント内で同一デジタルコンテンツに対して複数権利情報ファイルが存在する場合、権利情報ファイルはそれぞれ独立に扱われており、権利情報ファイル同士のクライアント内での結合を行うことができなかった。そのため、権利情報ファイルはその個数分だけ存在し、ユーザが単一コンテンツを利用する場合でも、権利の選択をする必要があった。

【0008】

本発明は、前記実情に鑑みてなされたものであり、複数権利の組み合わせによる権利表現を可能とし、より柔軟な権利表現が可能となる情報処理装置及び情報処理方法、並びに情報処理システムの提供を目的とする。

【0009】

【課題を解決するための手段】

本発明に係る情報処理装置は、前記課題を解決するために、ライセンス情報に記された使用条件の範囲内でコンテンツ情報を使用可能な情報処理装置において、第1のライセンス情報を保存する保存手段と、第2のライセンス情報を受信する受信手段と、第1のライセンス情報に対して第2のライセンス情報の一部又は全部を結合する結合手段とを有し、前記結合手段により結合されたライセンス情報の範囲内でコンテンツ情報を使用する。

【0010】

本発明の情報処理装置は、結合手段により第1のライセンス情報に対して第2のライセンス情報の一部又は全部を結合し、その結合した結果のライセンス情報に基づいてコンテンツ情報を使用する。

【0011】

本発明に係る情報処理方法は、前記課題を解決するために、ライセンス情報に記された使用条件の範囲内でコンテンツ情報を使用可能とする情報処理方法において、第1のライセンス情報を保存する保存工程と、第2のライセンス情報を受

信する受信工程と、前記受信工程で受信した第2のライセンス情報が上書きのためのライセンス情報であるか、追加のためのライセンス情報であることを識別させるライセンス識別情報から上書き又は追加属性を判別する判別工程と、前記判別工程で判別した上書き又は追加属性に応じて第1のライセンス情報に対して第2のライセンス情報の一部又は全部を結合する結合工程とを有し、前記結合工程により結合されたライセンス情報の範囲内でコンテンツ情報を使用する。

【0012】

本発明の情報処理方法は、結合工程により第1のライセンス情報に対して第2のライセンス情報の一部又は全部を結合し、その結合した結果のライセンス情報に基づいてコンテンツ情報を使用する。

【0013】

本発明に係る情報処理システムは、前記課題を解決するために、第1のライセンス情報を保存する保存手段と、第2のライセンス情報を受信する受信手段と、第1のライセンス情報に対して第2のライセンス情報の一部又は全部を結合する結合手段とを有し、前記結合手段により結合されたライセンス情報の範囲内でコンテンツ情報を使用するクライアントと、前記クライアントからの要求に応じて前記第2のライセンス情報をネットワークを通して送信するサーバとを備える。

【0014】

本発明の情報処理システムでは、クライアントの保存手段に保存されている第1のライセンス情報に対して、クライアントからの要求に応じてサーバから送信された第2のライセンス情報の一部又は全部を結合し、その結合した結果のライセンス情報に基づいてクライアントがコンテンツ情報を使用する。

【0015】

以上の本発明によれば、ライセンス情報を格納している権利ファイルにクライアント内での結合属性を指定可能とするとともに、その中で指定される各種権利情報に関しても属性に応じた結合ルールを設けるので、それにより複数権利ファイルをクライアント内で結合し単一権利としての利用を可能にする。

【0016】

【発明の実施の形態】

図1は、本発明を適用したコンテンツ提供システム1の構成を示している。コンテンツ提供システム1は、映像及び／音声データよりなるデータを扱う。サーバ11は、インターネットのようなネットワーク2を介してクライアント12に接続している。ここでは、クライアント12を一台のみ図示しているが、インターネット2には、任意の台数のクライアント12が接続される。

【0017】

クライアント12は、後述するライセンス情報に記された使用条件の範囲内でコンテンツ情報を使用可能な情報処理装置であり、既存（第1の）ライセンス情報を記憶部に記憶している。また、新規（第2の）ライセンス情報を通信部にて受信し、既存（第1の）ライセンス情報に対して新規（第2の）ライセンス情報の一部又は全部を結合する。この結合されたライセンス情報の範囲内でコンテンツ情報を使用する。

【0018】

ここでいうライセンス情報の結合は、後述するライセンス情報の更新の一形態としてなされる。

【0019】

なお、第2のライセンス情報は、自身が上書きのためのライセンス情報であるか、追加のためのライセンス情報であるかを識別可能なライセンス識別情報を含んでいる。

【0020】

また、サーバ11は、クライアント12に対してコンテンツを提供するほか、上記コンテンツを利用するのに必要なライセンス情報を付与する。また、課金処理を行うこともある。

【0021】

このコンテンツ提供システムは、詳細には図2に示すように記述することもできる。つまり、インターネット2には、クライアント12-1，12-2（以下、これらのクライアントを個々に区別する必要がある場合、単にクライアント12と称する）が接続されている。もちろん、インターネット2には、前述したように任意の台数のクライアントが接続される。また、インターネット2には、ク

クライアント 1 2 に対してコンテンツを提供するコンテンツサーバ 1 1 - A、コンテンツサーバ 1 1 - A が提供するコンテンツを利用するのに必要なライセンスをクライアント 1 2 に対して付与するライセンスサーバ 1 1 - B、およびクライアント 1 2 がライセンスを受け取った場合に、そのクライアント 1 2 に対して課金処理を行う課金サーバ 1 1 - C が接続されている。

【 0 0 2 2 】

図 3 はクライアント 1 2 の構成を表している。図 3 において、C P U (Central Processing Unit) 2 1 は、R O M (Read Only Memory) 2 2 に記憶されているプログラム、または記憶部 2 8 から R A M (Random Access Memory) 2 3 にロードされたプログラムに従って各種の処理を実行する。タイマ 2 0 は、計時動作を行い、時刻情報を C P U 2 1 に供給する。R A M 2 3 にはまた、C P U 2 1 が各種の処理を実行する上において必要なデータなども適宜記憶される。

【 0 0 2 3 】

暗号化復号部 2 4 は、コンテンツデータを暗号化するとともに、既に暗号化されているコンテンツデータを復号する処理を行う。コーデック部 2 5 は、例えば、A T R A C (Adaptive Transform Acoustic Coding) 3 方式などでコンテンツデータをエンコードし、入出力インタフェース 3 2 を介してドライブ 3 0 に接続されている半導体メモリ 4 4 に供給し、記録させる。あるいはまた、コーデック部 2 5 は、ドライブ 3 0 を介して半導体メモリ 4 4 より読み出した、エンコードされているデータをデコードする。半導体メモリ 4 4 は、いわゆるメモリーカードとして用いられているものである。

【 0 0 2 4 】

C P U 2 1、R O M 2 2、R A M 2 3、暗号化復号部 2 4、およびコーデック部 2 5 は、バス 3 1 を介して相互に接続されている。このバス 3 1 にはまた、入出力インタフェース 3 2 も接続されている。

【 0 0 2 5 】

入出力インタフェース 3 2 には、キーボード、マウスなどよりなる入力部 2 6、C R T、L C D などよりなるディスプレイ、並びにスピーカなどよりなる出力部 2 7、ハードディスクなどより構成される記憶部 2 8、モデム、ターミナルア

ダブタなどより構成される通信部 2 9 が接続されている。

【 0 0 2 6 】

通信部 2 9 は、インターネット 2 を介しての通信処理を行う。CPU 2 1 から提供されたデータを送信する。また通信部 2 9 は通信相手から受信したデータを CPU 2 1、RAM 2 3、記憶部 2 8 に出力する。記憶部 2 8 は CPU 2 1 との間でやり取りし、情報の保存・消去を行う。通信部 2 9 はまた、他のクライアントとの間で、アナログ信号またはデジタル信号の通信処理を行う。

【 0 0 2 7 】

入出力インタフェース 3 2 にはまた、必要に応じてドライブ 3 0 が接続され、磁気ディスク 4 1、光ディスク 4 2、光磁気ディスク 4 3、或いは半導体メモリ 4 4 などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部 2 8 にインストールされる。

【 0 0 2 8 】

なお、図示は省略するが、コンテンツサーバ 1 1 - A、ライセンスサーバ 1 1 - B、課金サーバ 1 1 - C も、図 3 に示したクライアント 1 2 と基本的に同様の構成を有するコンピュータにより構成される。そこで、以下の説明においては、図 3 の構成は、サーバ 1 1 の構成としても引用される。

【 0 0 2 9 】

コンテンツ提供システム 1 にあってサーバ 1 1 はクライアント 1 2 に、図 4 に示すようにコンテンツと共にライセンス情報を送る。クライアント 1 2 がコンテンツを再生するためにはライセンスが必要となる。

【 0 0 3 0 】

コンテンツは、図 5 に示すように、コンテンツ本体と鍵から構成され、コンテンツ本体は何重にも鍵が掛けられている。クライアント 1 2 側では、受け取ったコンテンツとライセンス情報を基に、コンテンツ本体を復号し再生する。ライセンス情報には、使用権利 UsageRight が記述されている。使用権利 UsageRight は、例えばコンテンツの再生期限、再生回数、或いは CD 等のメディアへのコピー回数、ポータブルデバイス (PD) へのチェックアウト回数等の各種使用条件を示す情報である。

【0031】

本実施の形態にあって、クライアント12は、ライセンス情報に記された使用条件の範囲内でコンテンツ情報を使用可能な情報処理装置であり、既存（第1の）ライセンス情報を記憶部28に記憶している。また、新規（第2の）ライセンス情報を通信部29にて受信する。既存（第1の）ライセンス情報に対して新規（第2の）ライセンス情報の一部又は全部をCPU21により結合する。このCPU21により結合されたライセンス情報の範囲内でコンテンツ情報を使用する。

【0032】

このため、クライアント12は、CPU21の制御の基に図6に示すような機能ブロックとして機能する。クライアントの通信機能120はサーバ11からのメッセージを受け取り、そのメッセージを管理機能121に渡す。また、管理機能121より受け取ったメッセージをサーバ11に送信する。暗号機能123は、サーバ11と共有している秘密鍵を用いてメッセージの暗号化・復号化を行う。管理機能122は一部、暗号機能123を用いてメッセージを生成・解析する。記憶装置124は、前記記憶部28に相当し、既存（第1の）ライセンス情報を記憶している。また、結合された後のライセンス情報も記憶する。

【0033】

サーバ11は、CPU21の制御の基に図7に示すような機能ブロックにしたがって機能する。通信機能110はクライアント12からのメッセージを受け取り、そのメッセージを管理機能111に渡す。また、管理機能111より受け取ったメッセージをクライアント12に送信する。暗号機能113は、クライアントと共有している秘密鍵を用いてメッセージの暗号化・復号化を行う。管理機能111は、通信機能110を経由してクライアント12とメッセージを交換し、そのメッセージに応じた処理をする。また管理機能111は、一部暗号機能113を用いてメッセージを生成・解析する。処理装置112は、管理機能111より要求のあった処理を行う。

【0034】

次に、図8を参照して、前記ライセンス情報を格納している既存権利ファイル

と新規権利ファイルの簡略化したデータ構成を説明する。この既存権利ファイル又は新規権利ファイルのデータ構成は、一つのコンテンツ毎に設定される。また、一つのコンテンツに対して複数の権利ファイルも設定される。また、複数のコンテンツに対して一つの権利ファイルが設定されてもよい。

【 0 0 3 5 】

先ず、データネーム (Data Name) が記述される。その後に、ユーセージライトタイプ (Usage Right Type : 使用権利タイプ) が記述されている。以下、コンテンツ ID (C I D)、ユーセージライトディスジャンクションルール (Usage Right Disjunction Rules : 使用権利分離規則)、リーフ ID (Leaf I D : 端末 I D)、デバイスアンドメディアカテゴリーフォアチェックアウト (Devaice and Media Categories for Check Out : チェックアウトのための端末及び媒体のカテゴリー)、チェックアウトマックスカウント (Check Out Max Count : チェックアウトの最大回数)、デバイスアンドメディアカテゴリーフォアコピー (Devaice and Media Categories for copy : コピーのための端末及び媒体のカテゴリー)、コピーマックスカウント (Copy Out Max Count : コピーの最大回数) が記述されている。また、アトラック 3 C D バーンマックスカウント (AT3CD Burn Max Count : 符号化方式アトラック 3 での C D への複写最大回数)、スタートタイム (start_time : 絶対開始時間)、エンドタイム (end_time : 絶対終了時間)、ピリオドタイム (period_time : 相対時間) も記述されている。これら各情報は、1 つの権利ファイルの中に全て記述されている必要はなく、どれか一つ、二つ、又はそれ以外の複数でもよい。もちろん、全ての記述でも構わない。複数の場合の例としては、後述のようにチェックアウトの P D を指定するフラグに、その回数を指定する回数情報が付随しているような場合である。

【 0 0 3 6 】

ユーセージライトタイプ (UsageRightType) には、当該既存権利ファイル又は新規権利ファイルが上書き属性であるか追加属性であるかを識別させるフラグが記述されている。さらに、この使用権利タイプ UsageRightType には、新規権利ファイルが期間制限を指定する権利内容を含む場合に、新規権利の相対期間を既存権利の絶対期間にどのように結合するかを決定する識別フラグも記述されている

。

【 0 0 3 7 】

コンテンツ I D は、この権利ファイル（既存権利又は新規権利ファイル）がどのコンテンツに対応しているかを示す識別コードである。同じ I D、すなわちこのコンテンツはどの権利ファイルに対応するかを示す識別コードはコンテンツファイルの中にも記述されている。もちろん、改竄されないように署名がついている。

【 0 0 3 8 】

ユーセージライトディスジャンクションルール（Usage Right Disjunction Rules）は、フラグによって可否で規定できるルールを相関なしに独立に記述している。つまり、この領域内に独立な条件をいくつか指定している。例えば、この領域に 4 バイト（byte）確保している。具体的には、ビット 0（bit 0）をビットレートの変換の可否に規定することができる。残りのビット 1 - 3 2 をリザーブ（Reserved）として、今後、可否だけを指定するようなルールの記述に用いる。

。

【 0 0 3 9 】

リーフ I D（Leaf I D）は、個々のデバイスの識別番号である。

【 0 0 4 0 】

デバイスアンドメディアカテゴリーフォアチェックアウト（Devaice and Media Categories for Check Out）は、クライアントからチェックアウト可能な機器を指定するために記述されている。チェックアウトは、クライアントからポータブル機器（P D）にコンテンツを転送することを意味する。よって、クライアントからコンテンツを転送できるポータブル機器を示すフラグである。例えば、インターネットに接続して音楽データを記録できるネット接続型のミニディスク記録再生装置、時計を有してタイマー機能を備えるポータブル機器、時計のないポータブル機器の 3 つのカテゴリを定義できる。チェックアウト可能であることをフラグ“1”で示すと、“1 1 0”は、クライアントからコンテンツを転送することができる P D は、ネット接続型のミニディスク記録再生装置とタイマー機能を備えるポータブル機器であることを指定していることになる。時計のないポー

ダブル機器にはチェックアウトできないことを意味する。なお、チェックアウトしたコンテンツをPDから元のクライアントに戻すことをチェックインという。クライアントからPDに一度チェックアウトしたコンテンツをチェックインによりまたクライアントに戻した後、再びチェックアウトすることも可能である。

【0 0 4 1】

チェックアウトマックスカウント (Check Out Max Count) は、前記デバイスアンドメディアカテゴリーフォアチェックアウト (Devaice and Media Categories for Check Out) にてチェックアウトを許可したポータブル機器に対して最大何回までチェックアウトできるかを示す回数指定の情報である。

【0 0 4 2】

デバイスアンドメディアカテゴリーフォアコピー (Devaice and Media Categories for copy) は、クライアントからコピー可能な機器を指定するために記述されている。コピーは、クライアントからポータブル機器 (PD) にコンテンツを複写することを意味する。よって、クライアントからコンテンツを複写できるポータブル機器を示すフラグである。前記デバイスアンドメディアカテゴリーフォアチェックアウト (Devaice and Media Categories for Check Out) にて説明したのと同様に、ミニディスク記録再生装置、時計を有してタイマー機能を備えるポータブル機器、時計のないポータブル機器の3つのカテゴリを定義できる。コピー可能であることをフラグ“1”で示すと、“1 1 0”は、クライアントからコンテンツをコピーすることができるPDは、ネット接続型のミニディスク記録再生装置とタイマー機能を備えるポータブル機器であることを指定していることになる。時計のないポータブル機器にはコピーを禁止している。

【0 0 4 3】

コピーマックスカウント (Copy Out Max Count) は、前記デバイスアンドメディアカテゴリーフォアコピー (Devaice and Media Categories for copy) にてコピーを許可したポータブル機器に対して最大何回までコピーできるかを示す回数指定の情報である。

【0 0 4 4】

アトラック3CDバーンマックスカウント (AT3CD Burn Max Count) は、コー

デック方式 A T R A C 3 による C D へのコンテンツの複写最大回数を指定する情報である。

【 0 0 4 5 】

スタートタイム (start_time : 絶対開始時間) はコンテンツの利用可能開始絶対日時を示し、エンドタイム (end_time : 絶対終了時間) はコンテンツの利用可能終了絶対日時を示す。よって、スタートタイム (start_time : 絶対開始時間) とエンドタイム (end_time : 絶対終了時間) により、コンテンツの利用できる絶対期間を指定する。

【 0 0 4 6 】

ピリオドタイム (period_time : 相対時間) は、ある特定の日時からどれくらいの期間コンテンツを利用できるかを示す情報である。

【 0 0 4 7 】

以上の各情報を分類すると、期間制限を指定する情報と、フラグを指定する情報と、回数を指定する情報とに分けられる。期間制限を指定する情報は、スタートタイム (start_time : 絶対開始時間) とエンドタイム (end_time : 絶対終了時間) とピリオドタイム (period_time : 相対時間) である。

【 0 0 4 8 】

フラグを指定する情報は、ユーセージライトディスジャンクションルール (Usage Right Disjunction Rules) とデバイスアンドメディアカテゴリーフォアチェックアウト (Devaice and Media Categories for Check Out) とデバイスアンドメディアカテゴリーフォアコピー (Devaice and Media Categories for copy) である。

【 0 0 4 9 】

回数を指定する情報は、チェックアウトマックスカウント (Check Out Max Count) とコピーマックスカウント (Copy Out Max Count) とアトラック 3 C D バーンマックスカウント (AT3CD Burn Max Count) である。

【 0 0 5 0 】

以上に説明したライセンス情報の既存又は新規権利ファイルは、それぞれ前記ユーセージライトタイプ (Usage Right Type) のフラグにより、上書き属性であ

るか、追加属性であるが識別される。上書き属性は、既存権利ファイルに新規権利ファイルが結合されるとき（例えば権利ファイルの更新の際に）、既存権利ファイルの内容の上に新規権利ファイルのライセンス情報を上書きしてしまうという属性を示す。追加属性は、既存権利ファイルに新規権利ファイルが結合されるとき（例えば権利ファイルの更新の際に）、既存権利ファイルのライセンス情報に新規ファイルのライセンス情報を追加するという属性を示す。

【 0 0 5 1 】

以下、クライアント 1 2 が既に所有している一つの既存権利ファイルに、ライセンスサーバ 1 1 - B から新規権利ファイルを結合する際のいくつかの処理を、実施例 1、実施例 2、実施例 3、実施例 4 として説明する。

【 0 0 5 2 】

実施例 1

クライアント 1 2 は、ライセンスサーバ 1 1 - B から送信された新規権利の属性を、前記ユーセージライトタイプ (Usage Right Type) のフラグにより、確認する。前記フラグの確認により、新規権利の属性が上書き属性である場合、既存権利で指定する全ての権利情報を新規権利の内容で書き換える。また、クライアント 1 2 が内部的に保持している既存権利に対する状態情報（現在利用状況）も消去する。

【 0 0 5 3 】

前記ユーセージライトタイプ (Usage Right Type) のフラグの確認により、新規権利の属性が追加属性の場合、クライアント 1 2 における既存権利の情報は失われることなく、値が規則に従い追加される。また、クライアント 1 2 が内部的に保持している既存権利に対する状態情報（現在利用状況）は保持され、結合により生成された権利に対する状態情報として処理される。

【 0 0 5 4 】

実施例 2

クライアント 1 2 による、前記ユーセージライトタイプ (Usage Right Type) のフラグの確認により、ライセンスサーバ 1 1 - B から送信された新規権利の属性が追加属性であり、その権利情報として、前記期間制限を指定する権利内容を

含む際、新規権利と既存権利が含む前提条件に応じて下記のような結合規則が適応される。

【0055】

先ず、結合規則 2-1（実施例 2 の 1 番目の結合規則）は以下ようになる。前提条件としては、既存権利が前記スタートタイム（start_time：絶対開始時間）とエンドタイム（end_time：絶対終了時間）により、絶対期間を指定するものであり、また新規権利も絶対期間を指定するときである。この場合、結合規則 2-1 としては、開始期限については、既存権利と新規権利双方の開始期限を比較し、日時が小さい方を結合結果の開始期限として採用する。但し、期限のどちらかが無期限を指定する場合、無期限を採用することとする。また、終了期限について、既存権利と新規権利双方の終了期限を比較し、日時が多きい方を結合結果の終了期限として採用する。但し、期限のどちらかが無期限を指定する場合、無期限を採用することとする。

【0056】

次に、結合規則 2-2（実施例 2 の 2 番目の結合規則）は以下ようになる。前提条件としては、既存権利が前記絶対期間を指定するものであり、新規権利が前記ピリオドタイム（period_time：相対時間）により相対期間を指定するときである。この場合の結合規則 2-2 としては、新規権利での相対期間の追加の足し算ルールによって、ケース 1 とケース 2 に分けることになる。このケース 1 とケース 2 の識別のためのフラグも、前記ユーセージライトタイプ（Usage Right Type）に記述されている。例えば、（Usage Right Type）の何ビット目かが“1”であるか否かによって識別させる。結合規則 2-2 のケース 1 は、新規権利の相対期間の開始日時をコンテンツデータのダウンロード日時とし、終了日時を前記開始日時に相対期間を足して算出し、相対期間による開始日時及び終了日時と、既存権利の開始日時及び終了日時とを比較し、開始日時については早い方を選択し、終了日時については遅い方を選択する。結合規則 2-2 のケース 2 は、相対期間の開始日時を既存権利の終了日時とする。もしも、既存権利の終了日が過ぎてしまっている場合には、相対期間の開始日時をダウンロード時とし、終了日時はその開始日時に相対期間を足した日時とする。

【 0 0 5 7 】

以上の結合規則 2 - 1 と結合規則 2 - 2 にしたがった期間の決定処理手順を図 9 に示す。既存権利はいずれも絶対期間である。ステップ S 2 0 1 にてクライアント 1 2 は、ライセンスサーバ 1 1 - B から送られた新規権利の権利ファイルの前記ユーセージライトタイプ (Usage Right Type) のフラグをチェックし、追加属性であるか、上書き属性であるかを確認する。上書き属性であれば、ステップ S 2 0 2 に進んで、既存権利に新規権利を上書きする。

【 0 0 5 8 】

ステップ S 2 0 1 のチェックにて追加属性を確認すると、ステップ S 2 0 3 に進んで新規権利の期間指定を判定する。これは、新規権利ファイルに記述されているのがスタートタイム (start_time : 絶対開始時間) とエンドタイム (end_time : 絶対終了時間) であるのか、或いはピリオドタイム (period_time : 相対時間) であるのかをチェックすることによって判定できる。ステップ S 2 0 4 にて判定の結果、絶対期間を指定するものであることを確認すると、ステップ S 2 0 5 に進み、既存権利と新規権利の開始日時と終了日時を比較する。そして、ステップ S 2 0 6 にて開始日時として早い方を選択し、また終了日時として遅い方を選択する。

【 0 0 5 9 】

ステップ S 2 0 4 の判定の結果、新規権利の期間指定が相対期間を指定するものであるときには、ステップ S 2 0 7 に進んで相対期間指定での足し算ルールの判定を、前記ユーセージライトタイプ (Usage Right Type) のフラグをチェックすることによって行う。前記フラグのチェックによりステップ S 2 0 8 にてケース 1 であることを確認すると、ステップ S 2 0 9 に進み、新規権利の相対期間の開始日時をコンテンツデータのダウンロード日時とし、終了日時を前記開始日時に相対期間を足して算出する。ステップ S 2 1 0 では、相対期間による開始日時及び終了日時と、既存権利の開始日時及び終了日時とを比較する。そして、ステップ S 2 1 1 にて開始日時については早い方を選択し、終了日時については遅い方を選択する。

【 0 0 6 0 】

ステップ S 2 0 8 にてケース 2 であることを確認すると、ステップ S 2 1 2 に進み、既存権利の絶対期間の終了日時の有効性を判定する。ステップ S 2 1 3 では、有効であるか無効であるかをチェックし、有効であることを確認できればステップ S 2 1 4 に進んで、既存権利の終了日時を、起点として終了日時を算出する。ステップ S 2 1 3 にて無効であることを確認すると、既存権利の終了日が過ぎてしまっていることになるので、ステップ S 2 1 5 にて相対期間の開始日時をダウンロード時とし、終了日時はその開始日時に相対期間を足した日時とする。

【 0 0 6 1 】

次に、結合規則 2 - 3（実施例 2 の 3 番目の結合規則）は、以下のようになる。前提条件としては、既存権利が前記相対期間を指定するものであり、新規権利が前記絶対期間を指定するときである。この場合の結合規則 2 - 3 としては、開始期限については、既存権利と新規権利双方の開始期限を比較し、日時が小さい方を結合結果の開始期限として採用する。但し、期限のどちらかが無期限を指定する場合、無期限を採用することとする。終了期限について、既存権利と新規権利双方の終了期限を比較し、日時が多きい方を結合結果の終了期限として採用する。但し、どちらかの期限が無期限を指定する場合、無期限を採用することとする。

【 0 0 6 2 】

次に、結合規則 2 - 4（実施例 2 の 4 番目の結合規則）は、以下のようになる。前提条件としては、既存権利及び新規権利とも相対期間を指定するときである。この結合規則 2 - 4 は、開始期限については、既存権利と新規権利双方の開始期限を比較し、日時が小さい方を結合結果の開始期限として採用する。但し、期限のどちらが無期限を指定する場合、無期限を採用することとする。終了期限について、既存権利と新規権利双方の開始期限に新規権利の相対期間で指定される期間を加算した結果を、既存権利の終了期限と比較する。計算結果が既存権利より大きければ、その値を結合結果の終了期限として採用する。計算結果が既存権利より小さければ、既存権利の終了期限を結合結果の終了期限として採用する。

【 0 0 6 3 】

実施例 3

クライアント 1 2 による、前記ユーセージライトタイプ (Usage Right Type) のフラグの確認により、ライセンスサーバ 1 1 - B から送信された新規権利の属性が追加属性であり、その権利情報として、前記ユーセージライトディスジャンクションルール (Usage Right Disjunction Rules) とデバイスアンドメディアカテゴリーフォアチェックアウト (Devaice and Media Categories for Check Out) とデバイスアンドメディアカテゴリーフォアコピー (Devaice and Media Categories for copy) のように、フラグを指定する権利内容を含む際には、結合規則としては、既存権利と新規権利で対応するフラグ値の論理和を計算し、その値を結合結果のフラグ値として採用する。

【 0 0 6 4 】

例えば、デバイスアンドメディアカテゴリーフォアチェックアウト (Devaice and Media Categories for Check Out) の具体例を挙げる。既存権利のフラグが “0 1 0” であり、クライアントからコンテンツをチェックアウトすることができる P D は、タイマー機能を備えるポータブル機器のみであるのに対して、新規権利のフラグが “1 0 0” であり、クライアントからコンテンツをチェックアウトすることができる P D は、ネット接続型のミニディスク記録再生装置のみであっても、フラグの論理和は “1 1 0” であるので、結合の結果、ネット接続型のミニディスク記録再生装置とタイマー機能を備えるポータブル機器の両方がチェックアウト可能となる。

【 0 0 6 5 】

実施例 4

クライアント 1 2 による、前記ユーセージライトタイプ (Usage Right Type) のフラグの確認により、ライセンスサーバ 1 1 - B から送信された新規権利の属性が追加属性であり、その権利情報として、回数を指定する権利内容を含む際、新規権利と既存権利が含む前提条件に応じて下記のような結合規則が適応される。

【 0 0 6 6 】

先ず、結合規則 4 - 1 (実施例 4 の 1 番目の結合規則) は以下になる。
前提条件としては、既存権利が 0 以上の有限整数であり、新規権利も 0 以上の有

限整数であるときである。この場合、結合規則 4 - 1 としては、既存権利と新規権利双方の回数値を加算した値を、結合結果の回数値として採用する。但し、計算結果がクライアントの扱える整数の範囲を超える場合は無制限を意味するものとする。例えば、チェックアウトマックスカウント (Check Out Max Count) を具体例に挙げて説明する。既存権利がチェックアウト最大回数を「1 0」とし、新規権利が「1 5」とするときには、結合の結果を「2 5」とする。ただし、クライアントの扱える整数が「2 2」までである場合は無制限を意味するものとする。

【 0 0 6 7 】

次に、結合規則 4 - 2 (実施例 4 の 2 番目の結合規則) は以下になる。前提条件としては、既存権利が無制限であり、新規権利が 0 以上の有限整数であるときである。この場合、結合規則 4 - 2 としては、無制限を結合結果の回数値として採用する。

【 0 0 6 8 】

次に、結合規則 4 - 3 (実施例 4 の 3 番目の結合規則) は以下になる。前提条件としては、既存権利が 0 以上の有限整数であり、新規権利が無制限であるときである。この場合、結合規則 4 - 3 としては、無制限を結合結果の回数値として採用する。

【 0 0 6 9 】

次に、結合規則 4 - 4 (実施例 4 の 4 番目の結合規則) は以下になる。前提条件としては、既存権利及び新規権利とも無制限であるときである。この場合、結合規則 4 - 4 としては、無制限を結合結果の回数値として採用する。

【 0 0 7 0 】

なお、クライアント 1 2 の要求によりサーバ 1 1 から権利ファイルを送るときには、サーバ 1 1 はサーバ 1 1 のみが持つ署名用秘密鍵 (PrivateKey) により署名している。そして、権利ファイル+サーバの証明書+署名の形式でクライアント 1 2 に送信される。クライアント 1 2 は公開されているサーバの公開鍵 (PublicKey) で署名を復号し、復号結果が権利ファイルと一致するかどうかで権利ファイルに不正が行われていないかどうかを検証する。

【 0 0 7 1 】

ここで、既存権利ファイルにも新規権利ファイルにもサーバ 1 1 による署名が付加されている。権利ファイル全部ではなく、一部の条件のみを書き換え、または追加した場合にはクライアントは、サーバのみが持つ署名用秘密鍵 (PrivateKey) を持っていないのでサーバ 1 1 と同じ署名はできない。そこで、クライアント 1 2 は、以下のようにして結合ファイルを安全に保存する。すなわち、各々の権利ファイルについてサーバの署名を検証した後、結合した権利ファイルをクライアントのみが持つ署名用秘密鍵 (PrivateKey) で署名して保存する。

【 0 0 7 2 】

以上に説明した実施例 1 ～実施例 4 を含め、本実施の形態のコンテンツ提供システムによれば、既存の権利表現に比べ、複数権利の組み合わせによる権利表現が可能になり、より柔軟な権利表現が可能となる。

【 0 0 7 3 】

次に、図 1 0 のフローチャートを参照して、クライアント 1 2 がコンテンツサーバ 1 1 - A からコンテンツの提供を受ける処理の詳細について説明する。

【 0 0 7 4 】

ユーザが、入力部 2 6 を操作することでコンテンツサーバ 1 1 - A に対するアクセスを指令すると、CPU 2 1 は、管理機能 1 2 1 によりステップ S 1 において、通信機能 1 2 0 である通信部 2 9 を制御し、インターネット 2 を介してコンテンツサーバ 1 1 - A にアクセスさせる。ステップ S 2 において、ユーザが、入力部 2 6 を操作して、提供を受けるコンテンツを指定すると、CPU 2 1 は、管理機能部 1 2 1 はこの指定情報を受け取り、通信部 2 9 から、インターネット 2 を介してコンテンツサーバ 1 1 - A に、指定されたコンテンツを通知する。図 1 1 のフローチャートを参照して後述するように、この通知を受けたコンテンツサーバ 1 1 - A は、暗号化されたコンテンツデータを送信してくるので、ステップ S 3 において、CPU 2 1 は、通信部 2 9 を介して、このコンテンツデータを受信すると、ステップ S 4 において、その暗号化されているコンテンツデータを記憶部 2 8 を構成するハードディスクに供給し、記憶させる。

【 0 0 7 5 】

次に、図 11 のフローチャートを参照して、クライアント 12 の以上の処理に対応するコンテンツサーバ 11-A のコンテンツ提供処理について説明する。なお、以下の説明において、図 3 のクライアント 12 の構成は、コンテンツサーバ 11-A の構成としても引用される。

【0076】

ステップ S 21 において、コンテンツサーバ 11-A の CPU 21 は、インターネット 2 から通信部 29 を介してクライアント 12 よりアクセスを受けるまで待機し、アクセスを受けたと判定したとき、ステップ S 22 に進み、クライアント 12 から送信されてきたコンテンツを指定する情報を取り込む。このコンテンツを指定する情報は、クライアント 12 が、図 10 のステップ S 2 において通知してきた情報である。

【0077】

ステップ S 23 において、コンテンツサーバ 11-A の CPU 21 は、記憶部 28 に記憶されているコンテンツデータの中から、ステップ S 22 の処理で取り込まれた情報で指定されたコンテンツを読み出す。CPU 21 は、ステップ S 24 において、記憶部 28 から読み出されたコンテンツデータを、暗号化復号部 24 に供給し、コンテンツキー Kc を用いて暗号化させる。

【0078】

記憶部 28 に記憶されているコンテンツデータは、コーデック部 25 により、既に ATRAC3 方式によりエンコードされているので、このエンコードされているコンテンツデータが暗号化されることになる。

【0079】

なお、もちろん、記憶部 28 に予め暗号化した状態でコンテンツデータを記憶させることができる。この場合には、ステップ S 24 の処理は省略することが可能である。

【0080】

次に、ステップ S 25 において、コンテンツサーバ 11-A の CPU 21 は、暗号化したコンテンツデータを伝送するフォーマットを構成するヘッダに、暗号化されているコンテンツを復号するのに必要なキー情報と、コンテンツを利用す

るのに必要なライセンスを識別するためのライセンス I D を付加する。そして、ステップ S 2 6 において、コンテンツサーバ 1 1 - A の C P U 2 1 は、ステップ S 2 4 の処理で暗号化したコンテンツと、ステップ S 2 5 の処理でキーとライセンス I D を付加したヘッダとをフォーマット化したデータを、通信部 2 9 から、インターネット 2 を介して、アクセスしてきたクライアント 1 2 に送信する。

【 0 0 8 1 】

図 1 2 は、このようにして、コンテンツサーバ 1 1 - A からクライアント 1 2 にコンテンツが供給される場合のフォーマットの構成を表している。同図に示されるように、このフォーマットは、ヘッダ (Header) とデータ (Data) とにより構成される。

【 0 0 8 2 】

ヘッダには、コンテンツ情報 (Content information) 、デジタル権利管理情報 (D R M (Digital Right Management) information) 、ライセンス I D (License ID) 、イネーブリングキーブロック (有効化キーブロック) (E K B (EnablingKey Block)) および、E K B から生成されたキー K E K B C を用いて暗号化されたコンテンツキー K c としてのデータ K E K B C (Kc) が配置されている。

【 0 0 8 3 】

コンテンツ情報には、データとしてフォーマット化されているコンテンツデータを識別するためのコンテンツ I D (C I D) 、そのコンテンツのコーデックの方式などの情報が含まれている。

【 0 0 8 4 】

デジタル権利管理情報 D R M には、コンテンツを使用するための使用権利 (Usage right/rules/status) 、U R L (Uniform Resource Locator) が配置されている。使用する権利には、図 8 に示したように、例えば、再生期限、コンテンツの再生回数、コピー回数、チェックアウト回数などが記述される。

【 0 0 8 5 】

U R L は、ライセンス I D で規定されるライセンスを取得するときアクセスするアドレス情報であり、図 2 のシステムの場合、具体的には、ライセンスを受け

るために必要なライセンスサーバ 1 1 - B のアドレスである。ライセンス ID は、データとして記録されているコンテンツを利用するとき必要とされるライセンスを識別するものである。

【 0 0 8 6 】

データは、任意の数の暗号化ブロック (Encryption Block) により構成される。各暗号化ブロックは、イニシャルベクトル (I V (Initial Vector))、シード (Seed)、およびコンテンツデータをキー $K'c$ で暗号化したデータ $E K'c(dat a)$ により構成されている。

【 0 0 8 7 】

キー $K'c$ は、次式により示されるように、コンテンツキー Kc と、乱数で設定される値 $Seed$ をハッシュ関数に適用して演算された値により構成される。

$$K'c = \text{Hash}(Kc, Seed)$$

イニシャルベクトル $I V$ とシード $Seed$ は、各暗号化ブロック毎に異なる値に設定される。

【 0 0 8 8 】

この暗号化は、コンテンツのデータを 8 バイト単位で区分して、8 バイト毎に行われる。後段の 8 バイトの暗号化は、前段の 8 バイトの暗号化の結果を利用して行われる C B C (Cipher Block Chaining) モードで行われる。

【 0 0 8 9 】

C B C モードの場合、最初の 8 バイトのコンテンツデータを暗号化するとき、その前段の 8 バイトの暗号化結果が存在しないため、最初の 8 バイトのコンテンツデータを暗号化するときは、イニシャルベクトル $I V$ を初期値として暗号化が行われる。

【 0 0 9 0 】

この C B C モードによる暗号化を行うことで、1 つの暗号化ブロックが解読されたとしても、その影響が、他の暗号化ブロックにおよぶことが抑制される。

【 0 0 9 1 】

以上のようにして、クライアント 1 2 は、コンテンツサーバ 1 1 - A からコンテンツを取得することができる。

【0092】

この取得したコンテンツの再生には、前記図8に示したようなライセンス情報を保持している必要がある。先ず、図13を参照して、クライアント12がコンテンツを再生する場合の処理について説明する。

【0093】

ステップS41において、クライアント12のCPU21は、ユーザが入力部26を操作することで指示したコンテンツの識別情報（CID）を取得する。この識別情報は、例えば、コンテンツのタイトルや、記憶されている各コンテンツ毎に付与されている番号などにより構成される。

【0094】

そして、CPU21は、コンテンツが指示されると、そのコンテンツに対応するライセンスID（そのコンテンツを使用するのに必要なライセンスのID）を読み取る。このライセンスIDは、図12に示されるように、暗号化されているコンテンツデータのヘッダに記述されているものである。

【0095】

次に、ステップS42に進み、CPU21は、ステップS41で読み取られたライセンスIDに対応するライセンスが、クライアント12により既に取得され、記憶部28に記憶されているか否かを判定する。まだ、ライセンスが取得されていない場合には、ステップS43に進み、CPU21は、ライセンス取得処理を実行する。このライセンス取得処理の詳細は、図14のフローチャートを参照して後述する。

【0096】

ステップS42において、ライセンスが既に取得されていると判定された場合、または、ステップS43において、ライセンス取得処理が実行された結果、ライセンスが取得された場合、ステップS44に進み、CPU21は、取得されているライセンスは有効期限内のものであるか否かを判定する。ライセンスが有効期限内のものであるか否かは、ライセンスの内容として規定されている期限と、タイマ20により計時されている現在日時と比較することで判断される。ライセンスの有効期限が既に満了していると判定された場合、CPU21は、ステップ

S 4 5に進み、ライセンス更新処理を実行する。このライセンス更新処理の詳細は、後述のフローチャートを参照して後述する。

【0097】

ステップS 4 4において、ライセンスはまだ有効期限内であると判定された場合、または、ステップS 4 5において、ライセンスが更新された場合、ステップS 4 6に進み、CPU 2 1は、暗号化されているコンテンツデータを記憶部 2 8から読み出し、RAM 2 3に格納させる。そして、ステップS 4 7において、CPU 2 1は、RAM 2 3に記憶された暗号化ブロックのデータを、図 1 2のデータに配置されている暗号化ブロック単位で、暗号化復号部 2 4に供給し、コンテンツキー K cを用いて復号させる。

【0098】

コンテンツキー K cを得る方法の具体例は、デバイスノードキー (DNK) を用いて、EKB (図 1 2) に含まれるキー K E K B Cを得ることができ、そのキー K E K B Cを用いて、データ K E K B C (K c) (図 1 2) から、コンテンツキー K cを得ることができる。

【0099】

CPU 2 1は、さらに、ステップS 4 8において、暗号化復号部 2 4により復号されたコンテンツデータをコーデック部 2 5に供給し、デコードさせる。そして、コーデック部 2 5によりデコードされたデータを、CPU 2 1は、入出力インタフェース 3 2から出力部 2 7に供給し、D/A変換させ、スピーカから出力させる。

【0100】

次に、図 1 4のフローチャートを参照して、図 1 3のステップS 4 3で行われるライセンス取得処理の詳細について説明する。

【0101】

クライアント 1 2は、事前にライセンスサーバ 1 1-Bに登録することにより、リーフ ID、DNK (Device Node Key)、クライアント 1 2の秘密鍵・公開鍵のペア、ライセンスサーバの公開鍵、及び各公開鍵の証明書を含むサービスデータを取得しておく。

【0102】

リーフIDは、クライアント毎に割り当てられた識別情報を表し、DNKは、そのライセンスに対応するEKB（有効化キープロック）に含まれる暗号化されているコンテンツキーKcを復号するのに必要なデバイスノードキーである。

【0103】

最初にステップS61において、CPU21は、いま処理対象とされているライセンスIDに対応するURLを、図12に示すヘッダから取得する。上述したように、このURLは、やはりヘッダに記述されているライセンスIDに対応するライセンスを取得するときアクセスすべきアドレスである。そこで、ステップS62において、CPU21は、ステップS61で取得したURLにアクセスする。具体的には、通信部29によりインターネット2を介してライセンスサーバ11-Bにアクセスが行われる。このとき、ライセンスサーバ11-Bは、クライアント12に対して、購入するライセンス（コンテンツを使用するのに必要なライセンス）を指定するライセンス指定情報、並びにユーザIDとパスワードの入力を要求してくる（後述する図16のステップS102）。CPU21は、この要求を出力部27の表示部に表示させる。ユーザは、この表示に基づいて、入力部26を操作して、ライセンス指定情報、ユーザID、およびパスワードを入力する。なお、このユーザIDとパスワードは、クライアント12のユーザが、インターネット2を介してライセンスサーバ11-Bにアクセスし、事前に取得しておいたものである。

【0104】

CPU21は、ステップS63、S64において、入力部26から入力されたライセンス識別情報を取り込むとともに、ユーザIDとパスワードを取り込む。CPU21は、ステップS65において、通信部29を制御し、入力されたユーザIDとパスワードを、ライセンス指定情報及びサービスデータ（後述する）に含まれるリーフIDを含むライセンス要求をインターネット2を介してライセンスサーバ11-Bに送信させる。

【0105】

ライセンスサーバ11-Bは、ユーザIDとパスワード、並びにライセンス指

定情報に基づいてライセンスを送信してくる（ステップS109）か、または、条件が満たされない場合には、ライセンスを送信してこない（ステップS112）。

【0106】

ステップS66において、CPU21は、ライセンスサーバ11-Bからライセンスが送信されてきたか否かを判定し、ライセンスが送信されてきた場合には、ステップS67に進み、そのライセンスを記憶部28に供給し、記憶させる。

【0107】

ステップS66において、ライセンスが送信されて来ないと判定した場合、CPU21は、ステップS68に進み、エラー処理を実行する。具体的には、CPU21は、コンテンツを利用するためのライセンスが得られないので、コンテンツの再生処理を禁止する。

【0108】

以上のようにして、各クライアント12は、コンテンツデータに付随しているライセンスIDに対応するライセンスを取得して、初めて、そのコンテンツを使用することが可能となる。

【0109】

なお、図14のライセンス取得処理は、各ユーザがコンテンツを取得する前に、予め行っておくようにすることも可能である。

【0110】

クライアント12に提供されるライセンスは、前記図8に示した権利ファイルを使用条件に含ませて、図15のように示される。

【0111】

次に、図16のフローチャートを参照して、図14のクライアント12のライセンス取得処理に対応して実行されるライセンスサーバ11-Bのライセンス提供処理について説明する。なお、この場合においても、図3のクライアント12の構成は、ライセンスサーバ11-Bの構成として引用される。

【0112】

ステップS101において、ライセンスサーバ11-BのCPU21は、クラ

クライアント 1 2 よりアクセスを受けるまで待機し、アクセスを受けたとき、ステップ S 1 0 2 に進み、アクセスしてきたクライアント 1 2 に対して、ユーザ ID とパスワード、並びに、ライセンス指定情報の送信を要求する。上述したようにして、クライアント 1 2 から、図 1 4 のステップ S 6 5 の処理で、ユーザ ID とパスワード、リーフ ID 並びにライセンス指定情報（ライセンス ID）が送信されてきたとき、ライセンスサーバ 1 1 - B の CPU 2 1 は、通信部 2 9 を介してこれを受信し、取り込む処理を実行する。

【 0 1 1 3 】

そして、ライセンスサーバ 1 1 - B の CPU 2 1 は、ステップ S 1 0 3 において、通信部 2 9 から課金サーバ 1 1 - C にアクセスし、ユーザ ID とパスワードに対応するユーザの与信処理を要求する。課金サーバ 1 1 - C は、インターネット 2 を介してライセンスサーバ 1 1 - B から与信処理の要求を受けると、そのユーザ ID とパスワードに対応するユーザの過去の支払い履歴などを調査し、そのユーザが、過去にライセンスの対価の不払いの実績があるか否かなどを調べ、そのような実績がない場合には、ライセンスの付与を許容する与信結果を送信し、不払いの実績などがある場合には、ライセンス付与の不許可の与信結果を送信する。

【 0 1 1 4 】

ステップ S 1 0 4 において、ライセンスサーバ 1 1 - B の CPU 2 1 は、課金サーバ 1 1 - C からの与信結果が、ライセンスを付与することを許容する与信結果であるか否かを判定し、ライセンスの付与が許容されている場合には、ステップ S 1 0 5 に進み、ステップ S 1 0 2 の処理で取り込まれたライセンス指定情報に対応するライセンスを、記憶部 2 8 に記憶されているライセンスの中から取り出す。記憶部 2 8 に記憶されているライセンスは、あらかじめライセンス ID、バージョン、作成日時、有効期限等の情報が記述されている。ステップ S 1 0 6 において、CPU 2 1 は、そのライセンスに受信したリーフ ID を付加する。さらに、ステップ S 1 0 7 において、CPU 2 1 は、ステップ S 1 0 5 で選択されたライセンスに対応づけられている使用条件を選択する。あるいはまた、ステップ S 1 0 2 の処理で、ユーザから使用条件が指定された場合には、その使用条件

が必要に応じて、予め用意されている使用条件に付加される。CPU 21は、選択された使用条件をライセンスに付加する。

【0115】

ステップS108において、CPU 21はライセンスサーバの秘密鍵によりライセンスに署名し、これにより、図15に示されるような構成のライセンスが生成される。

【0116】

次に、ステップS109に進み、ライセンスサーバ11-BのCPU 21は、そのライセンス（図15に示される構成を有する）を、通信部29からインターネット2を介してクライアント12に送信させる。

【0117】

ステップS110においてライセンスサーバ11-BのCPU 21は、ステップS109の処理で、いま送信したライセンス（使用条件、リーフIDを含む）を、ステップS102の処理で取り込まれたユーザIDとパスワードに対応して、記憶部28に記憶させる。さらに、ステップS111において、CPU 21は、課金処理を実行する。具体的には、CPU 21は、通信部29から課金サーバ11-Cに、そのユーザIDとパスワードに対応するユーザに対する課金処理を要求する。課金サーバ5は、この課金の要求に基づいて、そのユーザに対する課金処理を実行する。上述したように、この課金処理に対して、そのユーザが支払いを行わなかったような場合には、以後、そのユーザは、ライセンスの付与を要求したとしても、ライセンスを受けることができないことになる。

【0118】

すなわち、この場合には、課金サーバ11-Cからライセンスの付与を不許可とする与信結果が送信されてくるので、ステップS104からステップS112に進み、CPU 21は、エラー処理を実行する。具体的には、ライセンスサーバ11-CのCPU 21は、通信部29を制御してアクセスしてきたクライアント12に対して、ライセンスを付与することができない旨のメッセージを出力し、処理を終了させる。

【0119】

この場合、上述したように、そのクライアント12はライセンスを受けることができないので、そのコンテンツを利用すること（暗号を復号すること）ができないことになる。

【0120】

図17は、図13のステップS45におけるライセンス更新処理の詳細を表している。図17のステップS131乃至ステップS135の処理は、図15のステップS61乃至ステップS65の処理と基本的に同様の処理である。ただし、ステップS133において、CPU21は、購入するライセンスではなく、更新するライセンスのライセンスIDを取り込む。そして、ステップS135において、CPU21は、ユーザIDとパスワードとともに、更新するライセンスのライセンスIDを、ライセンスサーバ11-Bに送信する。

【0121】

ステップS135の送信処理に対応して、ライセンスサーバ11-Bは、後述するように、使用条件を提示してくる（図18のステップS153）。そこで、クライアント1のCPU21は、ステップS136において、ライセンスサーバ11-Bからの使用条件の提示を受信し、これを出力部27に出力し、表示させる。ユーザは、入力部26を操作して、この使用条件の中から所定の使用条件を選択したり、所定の使用条件を新たに追加したりする。ステップS137でCPU21は、以上のようにして選択された使用条件（ライセンスを更新する条件）を購入するための申し込みをライセンスサーバ11-Bに送信する。この申し込みに対応して、後述するようにライセンスサーバ11-Bは、最終的な使用条件を送信してくる（図18のステップS154）。そこで、ステップS138において、クライアント1のCPU21は、ライセンスサーバ11-Bからの使用条件を取得し、ステップS139において、その使用条件を記憶部28にすでに記憶されている対応するライセンスの使用条件として更新する。

【0122】

図18は、以上のクライアント12のライセンス更新処理に対応して、ライセンスサーバ11-Bが実行するライセンス更新処理を表している。

最初に、ステップS151において、ライセンスサーバ11-BのCPU21

は、クライアント 12 からのアクセスを受けると、ステップ S 152 において、クライアント 12 がステップ S 135 で送信したライセンス指定情報をライセンス更新要求情報とともに受信する。

【0123】

ステップ S 153 において、CPU 21 は、ライセンスの更新要求を受信すると、そのライセンスに対応する使用条件（更新する使用条件）を、記憶部 28 から読み出し、クライアント 12 に送信する。

【0124】

この提示に対して、上述したように、クライアント 12 から使用条件の購入が図 17 のステップ S 137 の処理で申し込まれると、ステップ S 154 において、ライセンスサーバ 11-B の CPU 21 は、申し込まれた使用条件に対応するデータを生成し、ステップ S 154 において、クライアント 12 に送信する。クライアント 12 は、上述したように、ステップ S 139 の処理で受信した使用条件を用いて、すでに登録されているライセンスの使用条件を更新する。

なお、本発明の情報処理装置が適用されるクライアントは、いわゆるパーソナルコンピュータ以外に、携帯情報端末（Personal Digital Assistants：PDA）、携帯電話機、ゲーム端末機などとすることができる。

【0125】

一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

【0126】

この記録媒体は、図 3 に示されるように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク 41（フロッピーディスクを含む）、光ディスク 42（CD-ROM (Compact Disk - Read Only Memory), DVD (Digital Versatile Disk) を含む）、光磁気ディスク 43（MD (Mini-Disk) を含む）、もしくは半導体メモリ 44 などよりなるパッケージ

メディアにより構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているROM22や、記憶部28に含まれるハードディスクなどで構成される。

【0127】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0128】

【発明の効果】

本発明に係る情報処理装置は、結合手段により第1のライセンス情報に対して第2のライセンス情報の一部又は全部を結合し、その結合した結果のライセンス情報に基づいてコンテンツ情報を使用するので、既存の権利表現に比べ、複数権利の組み合わせによる権利表現が可能になり、より柔軟な権利表現を可能とする。

【0129】

本発明に係る情報処理方法は、結合工程により第1のライセンス情報に対して第2のライセンス情報の一部又は全部を結合し、その結合した結果のライセンス情報に基づいてコンテンツ情報を使用するので、既存の権利表現に比べ、複数権利の組み合わせによる権利表現が可能になり、より柔軟な権利表現を可能とする。

【0130】

本発明に係る情報処理システムは、クライアントの保存手段に保存されている第1のライセンス情報に対して、クライアントからの要求に応じてサーバから送信された第2のライセンス情報の一部又は全部を結合し、その結合した結果のライセンス情報に基づいてクライアントがコンテンツ情報を使用するので、クライアント側では既存の権利表現に比べ、複数権利の組み合わせによる権利表現が可能になり、より柔軟な権利表現を可能とする。

【図面の簡単な説明】

【図1】

コンテンツ提供システムの一実施形態の構成図である。

【図 2】

コンテンツ提供システムの一実施形態の詳細な構成図である。

【図 3】

クライアントの構成を示す図である。

【図 4】

サーバからクライアントへのコンテンツとライセンスの送信を示す図である。

【図 5】

コンテンツとライセンスの関係を示す図である。

【図 6】

クライアントの機能ブロック図である。

【図 7】

サーバの機能ブロック図である。

【図 8】

既存又は新規権利ファイルの構成を示す図である。

【図 9】

実施例 2 の結合規則 2 - 1 と結合規則 2 - 2 にしたがった期間の決定処理手順を示すフローチャートである。

【図 1 0】

クライアントのコンテンツのダウンロード処理を説明するためのフローチャートである。

【図 1 1】

コンテンツサーバのコンテンツ提供処理を説明するためのフローチャートである。

【図 1 2】

コンテンツサーバからクライアントにコンテンツが供給される場合のコンテンツのフォーマット図である。

【図 1 3】

クライアントのコンテンツ再生処理を説明するためのフローチャートである。

【図 1 4】

クライアントのライセンス取得処理を説明するためのフローチャートである。

【図 15】

ライセンスの構成を示す図である。

【図 16】

ライセンスサーバのライセンス提供処理を説明するためのフローチャートである。

【図 17】

クライアントのライセンス更新処理を説明するためのフローチャートである。

【図 18】

ライセンスサーバのライセンス更新処理を説明するためのフローチャートである。

【符号の説明】

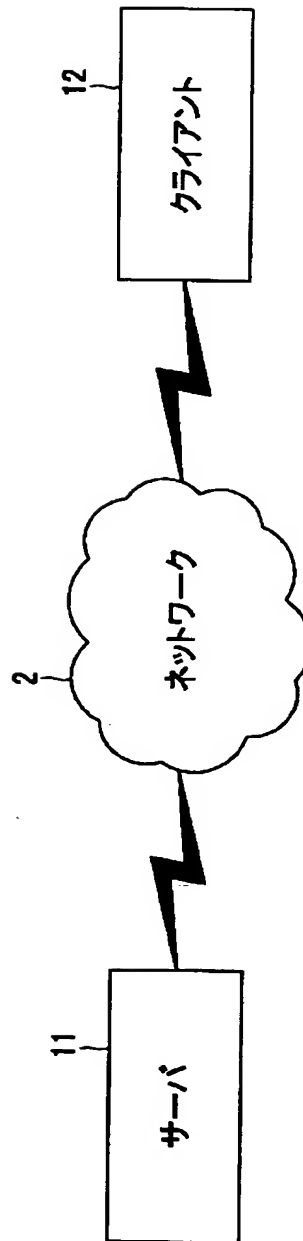
1 コンテンツ提供システム、2 ネットワーク、12 クライアント、21 CPU、28 記憶部、29 通信部

【書類名】

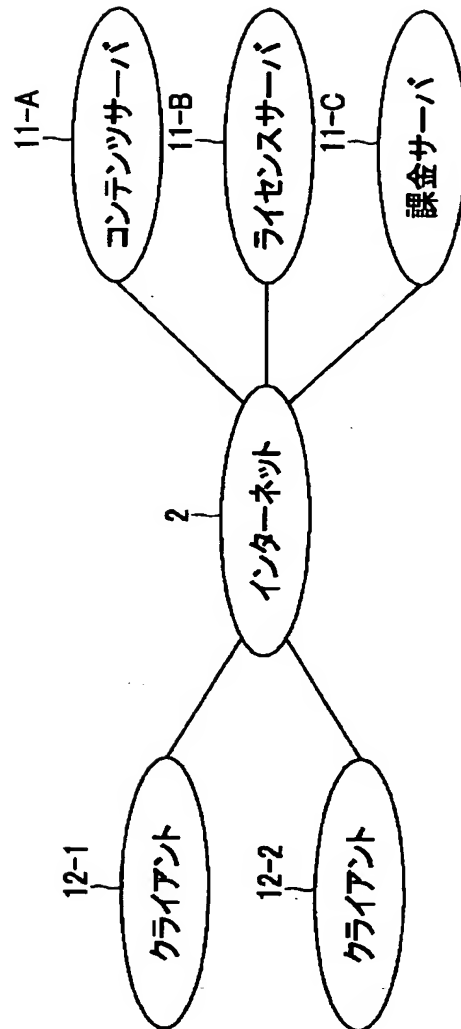
図面

【図 1】

1

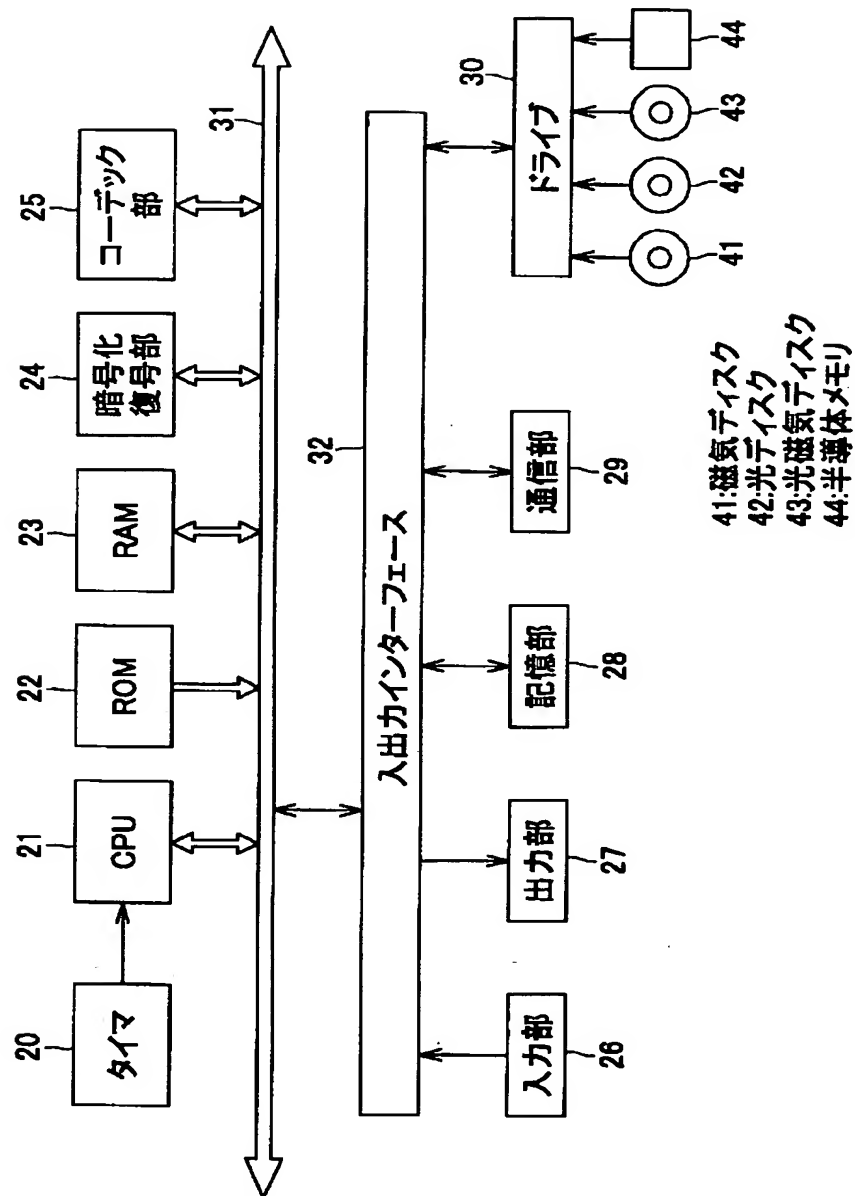


【図 2】

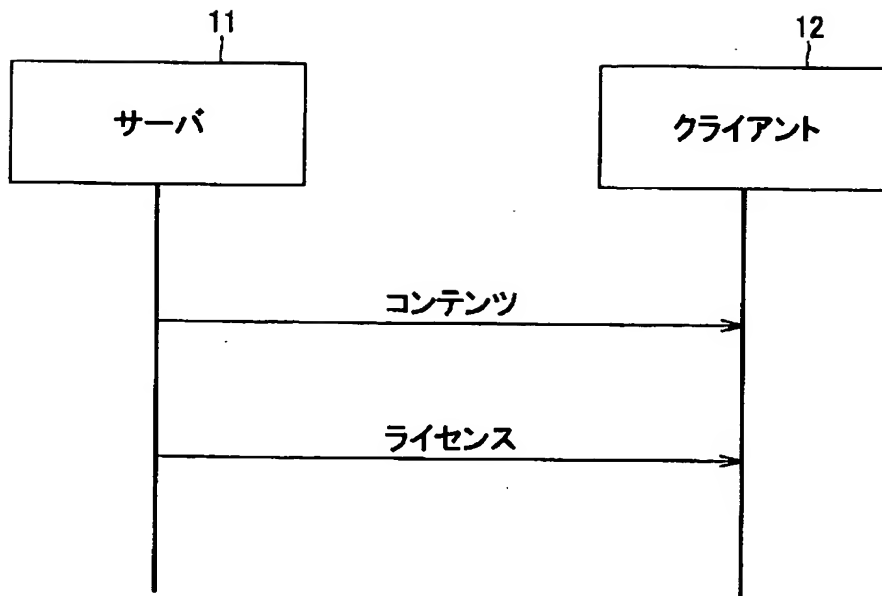


【図 3】

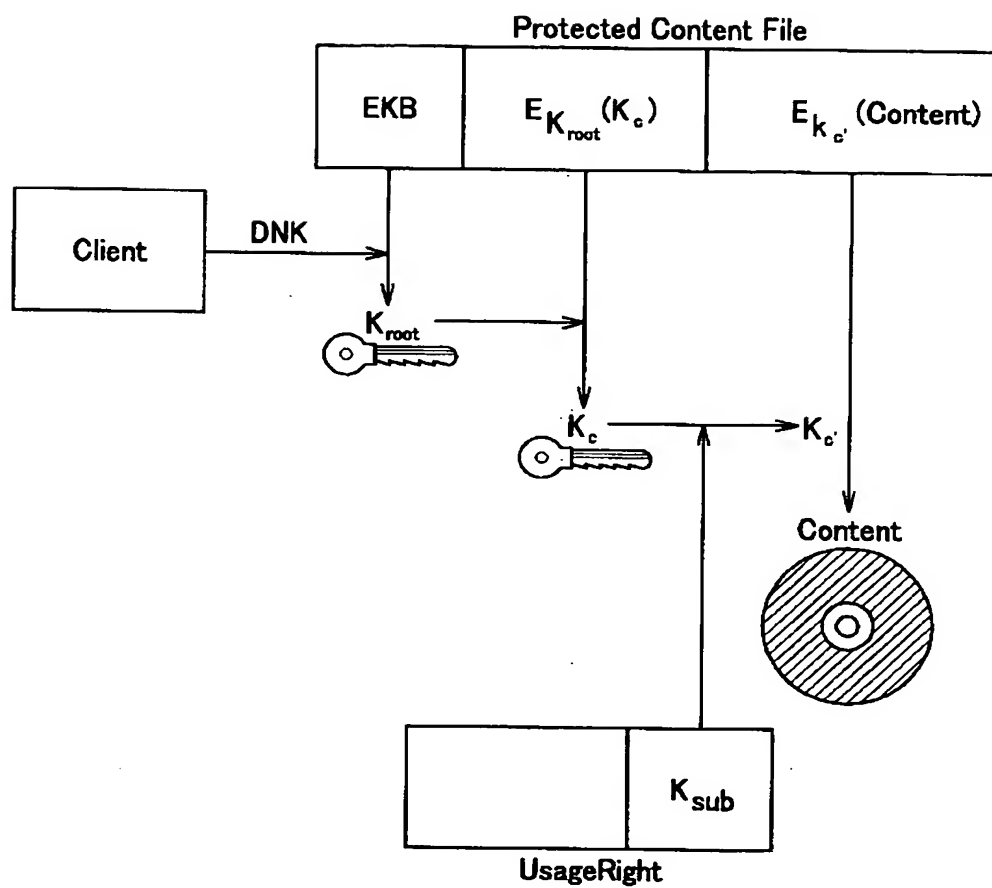
12



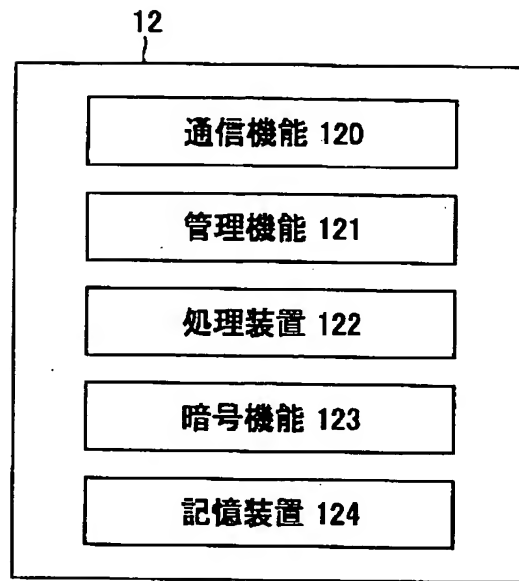
【図 4】



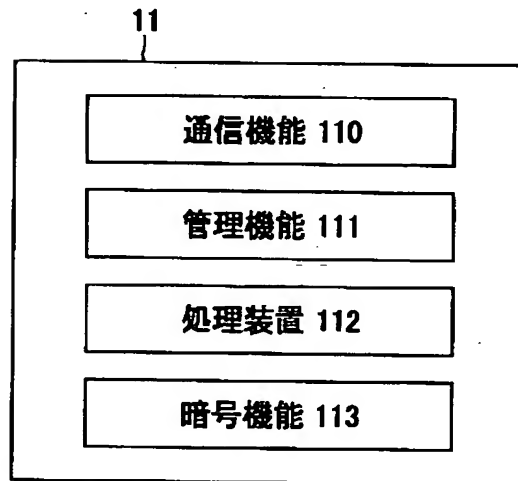
【図 5】



【図 6】



【図 7】

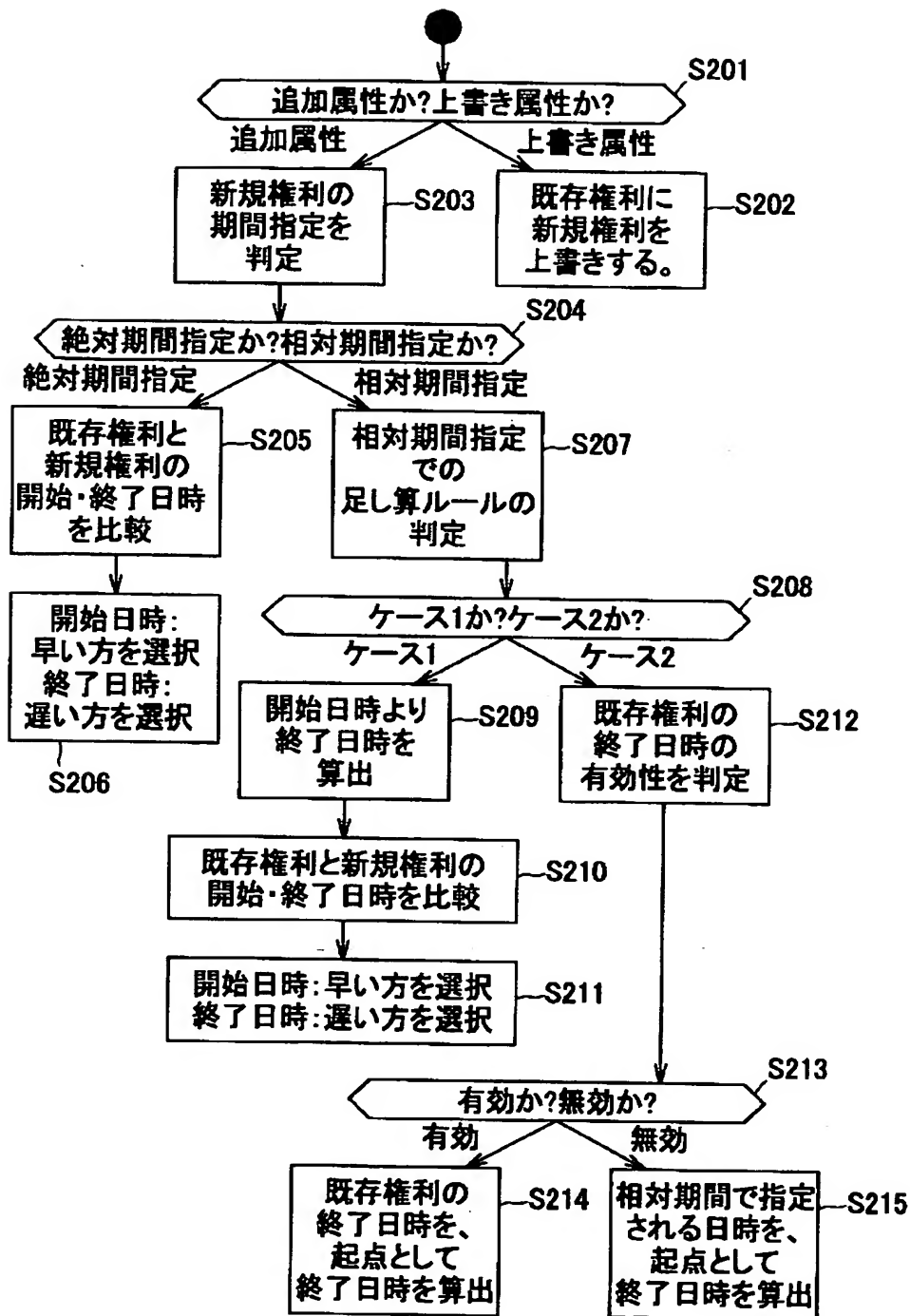


【図 8】

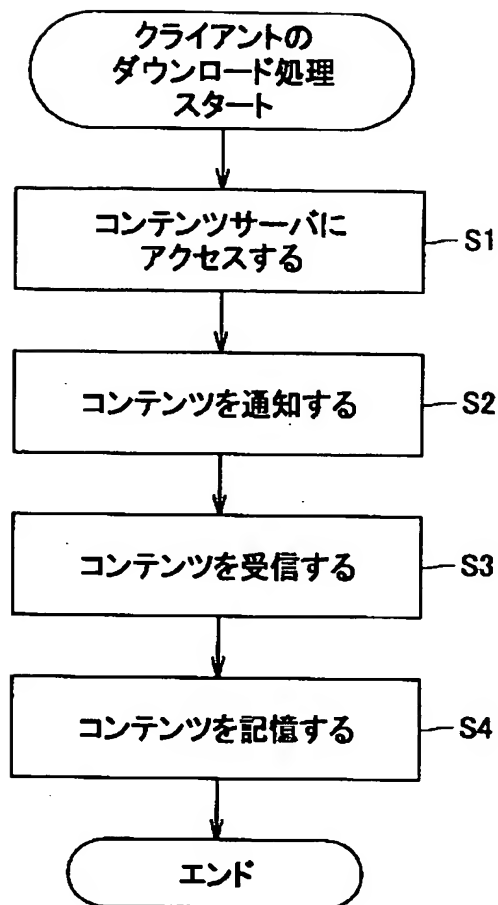
Data Name

UsageRightType
CID
UsageRight Disjunction Rules
Leaf ID
Device and Media Categories for Check Out
Check Out Max Count
Device and Media Categories for copy
Copy Max Count
AT3CD Burn Max Count
start_time
end_time
period_time

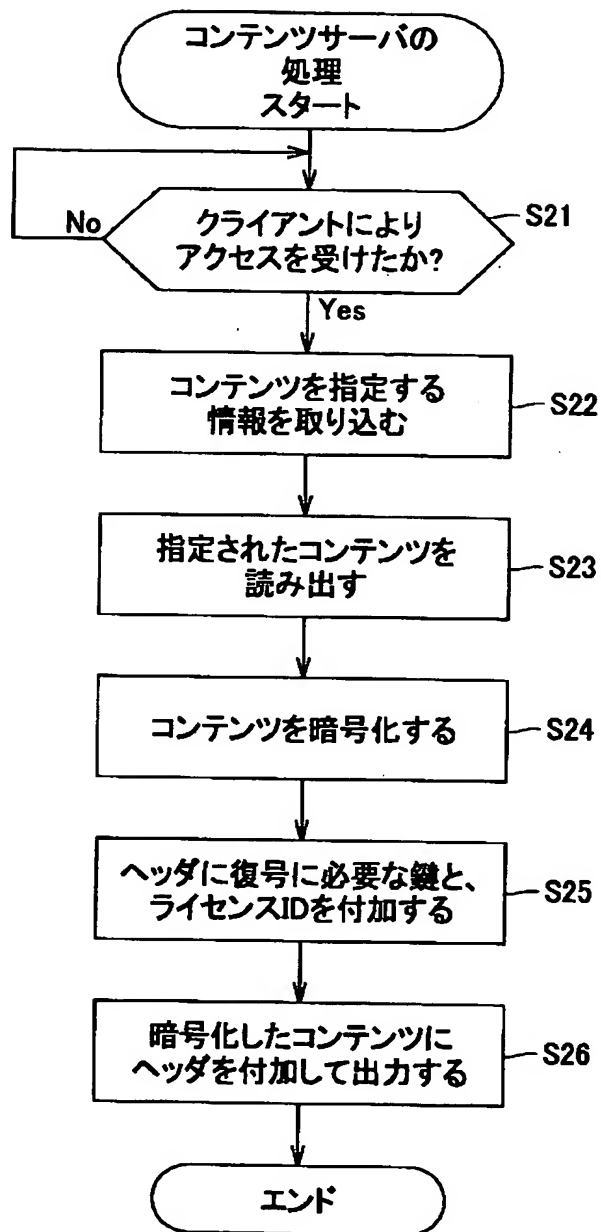
【図 9】



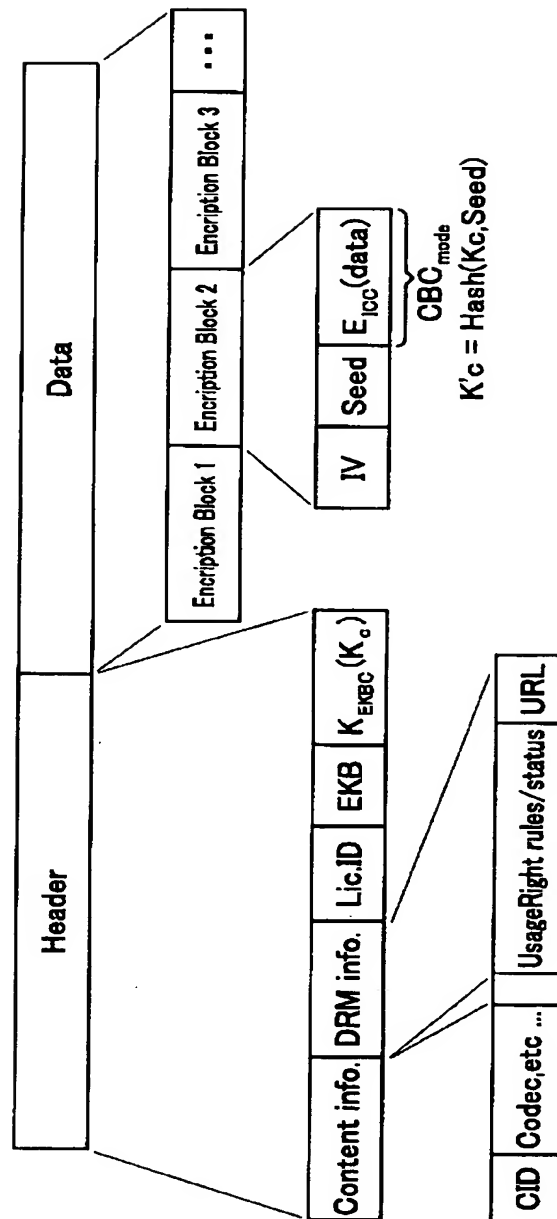
【図 10】



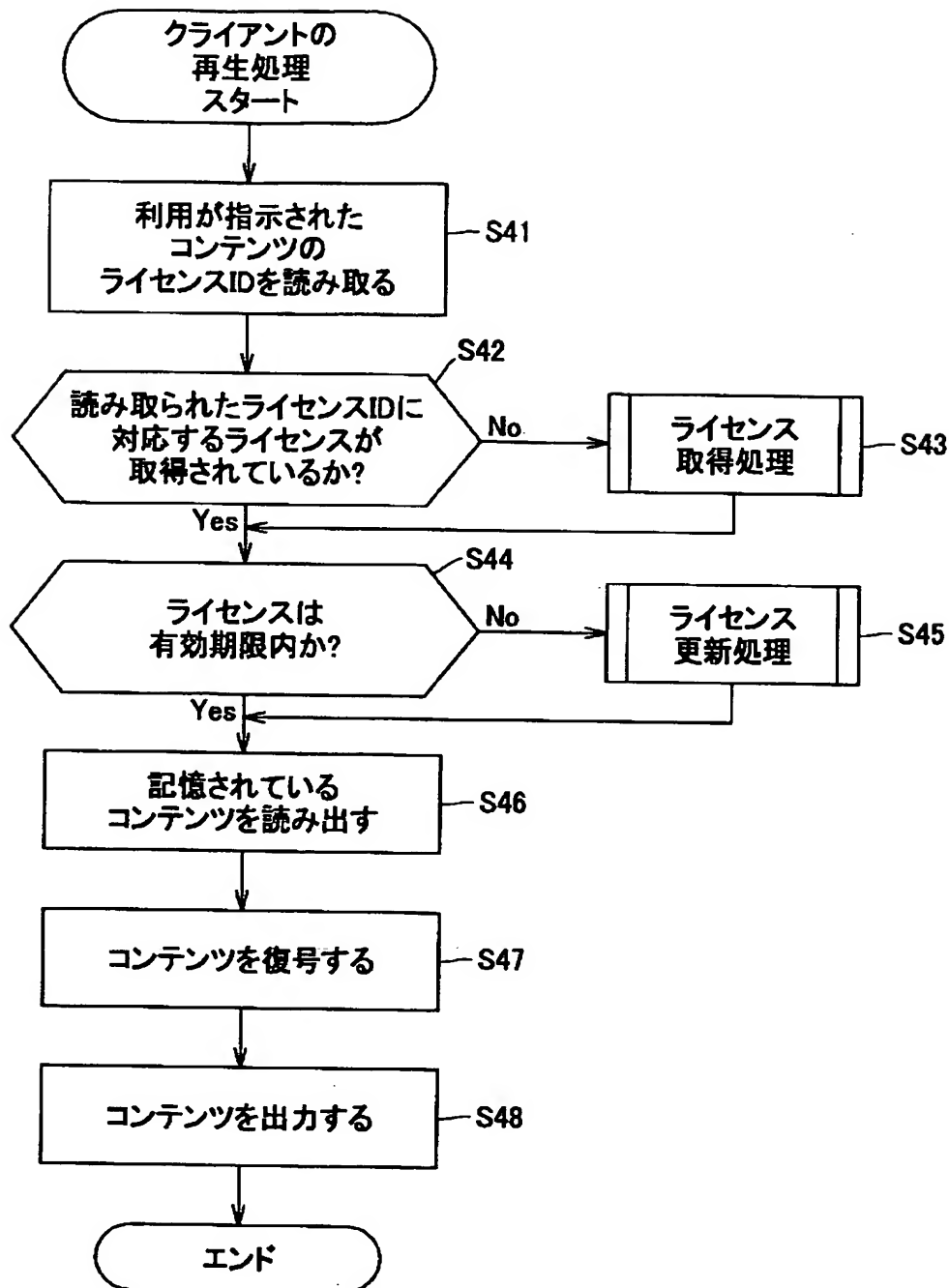
【図 11】



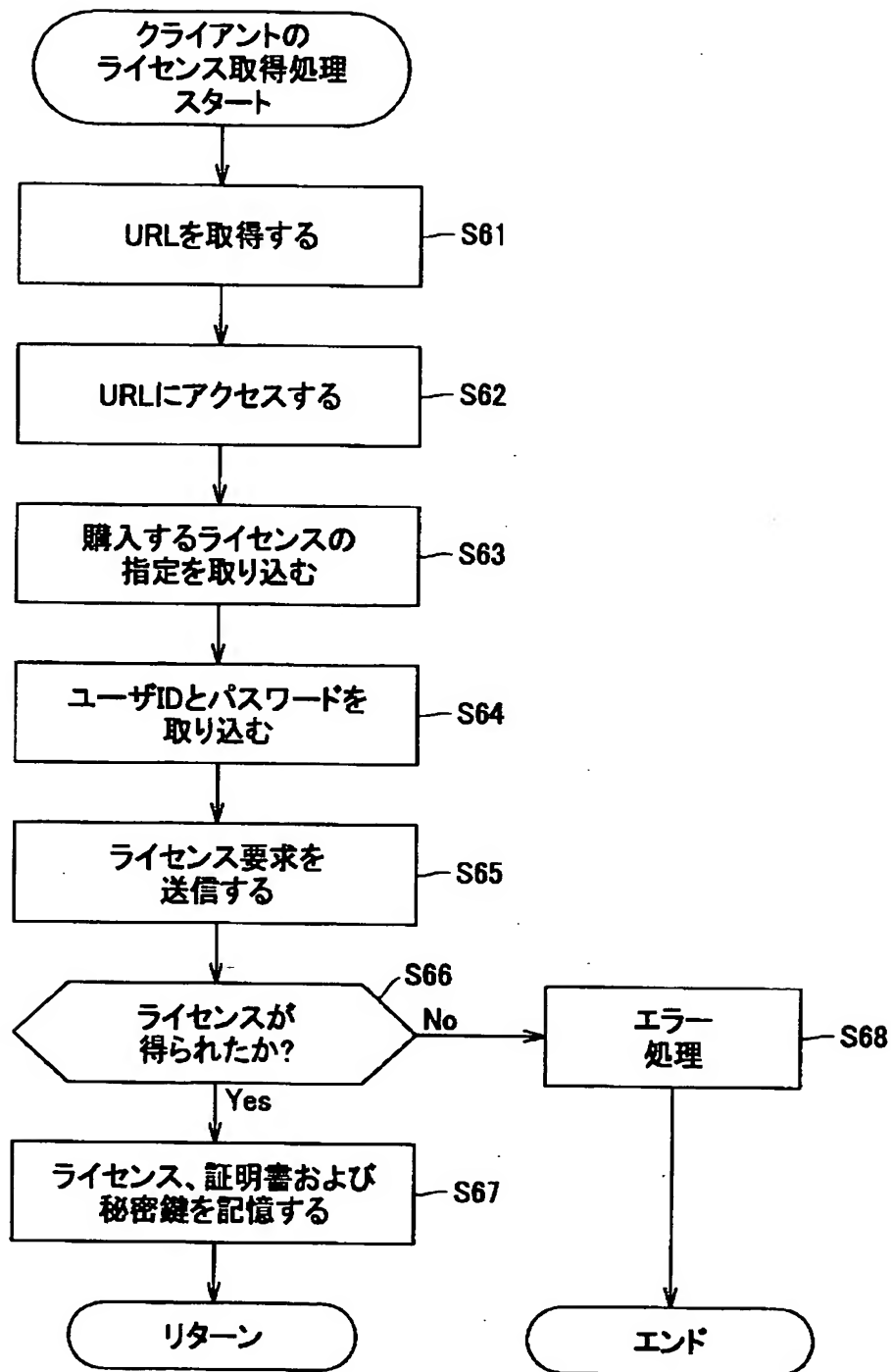
【図 1 2】



【図 13】



【図 14】

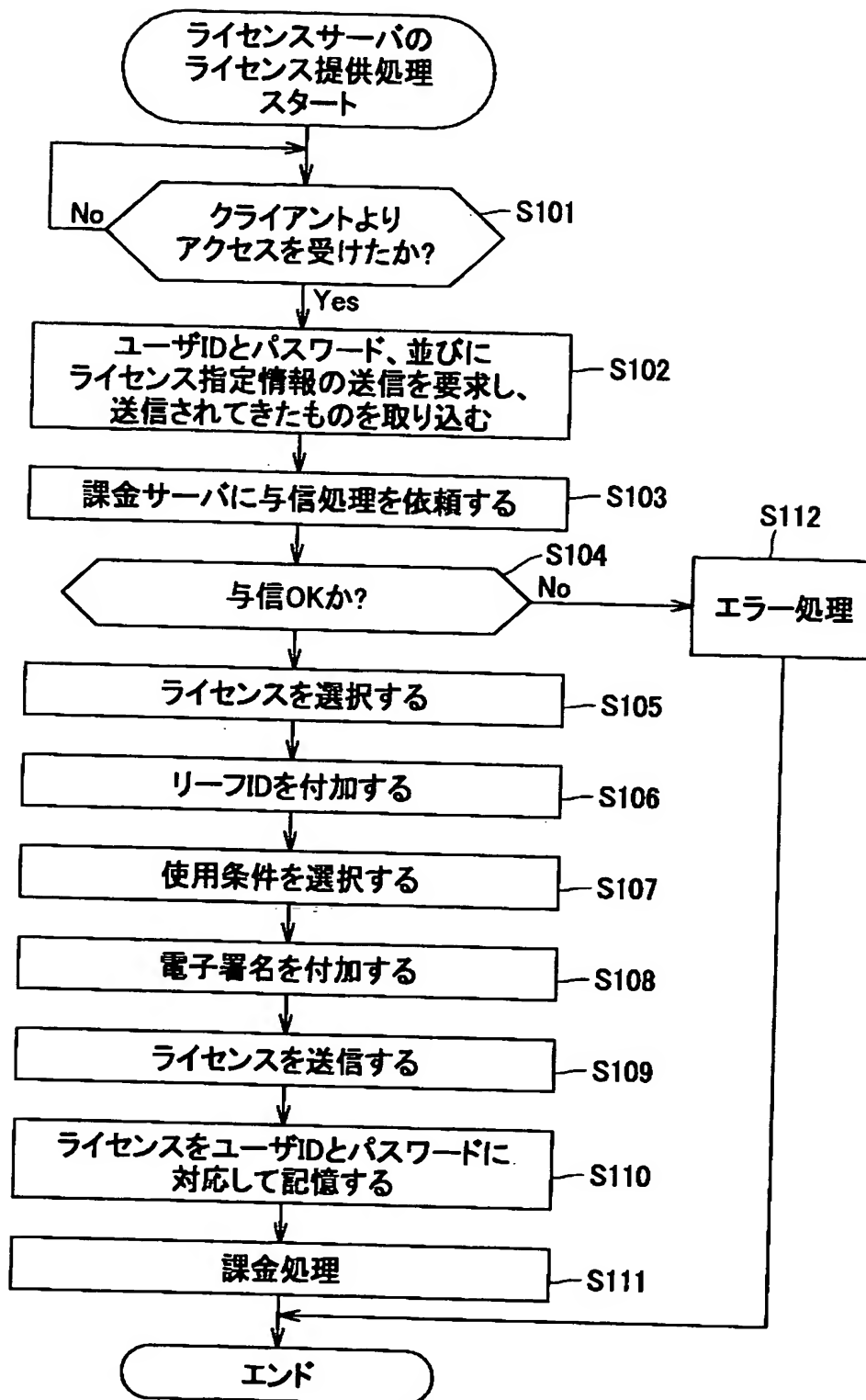


【図 15】

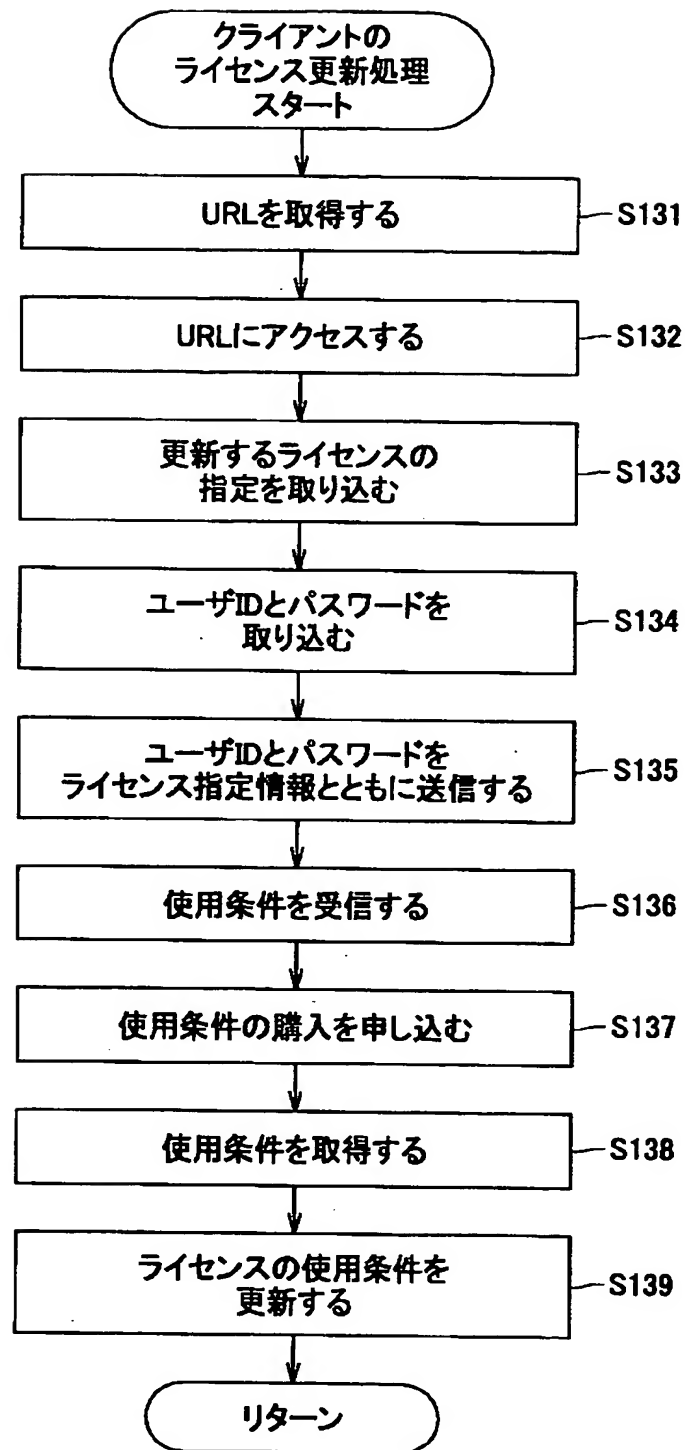
ライセンスID
作成日時
有効期限
使用条件
リーフ ID
電子署名

ライセンス

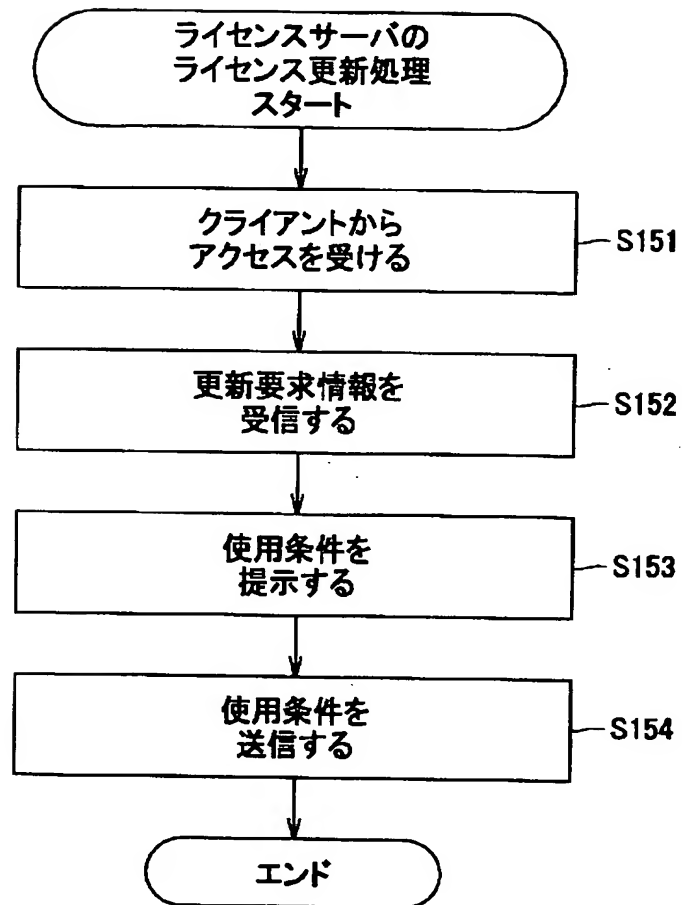
【図 16】



【図 17】



【図 18】



【書類名】 要約書

【要約】

【課題】 複数権利の組み合わせによる権利表現を可能とし、より柔軟な権利表現が可能とする。

【解決手段】 クライアント 1 2 は、ライセンス情報に記された使用条件の範囲内でコンテンツ情報を使用可能な情報処理装置であり、既存（第 1 の）ライセンス情報を記憶部 2 8 に記憶している。また、新規（第 2 の）ライセンス情報を通信部 2 9 にて受信し、既存（第 1 の）ライセンス情報に対して新規（第 2 の）ライセンス情報の一部又は全部を結合する。この結合されたライセンス情報の範囲内でコンテンツ情報を使用する。

【選択図】 図 3



特願 2 0 0 3 - 1 4 2 5 9 3

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 2 1 8 5]

1. 変更年月日	1 9 9 0 年 8 月 3 0 日
[変更理由]	新規登録
住 所	東京都品川区北品川 6 丁目 7 番 3 5 号
氏 名	ソニー株式会社